CHAPTER 5

Configuring Interfaces

This chapter describes how to configure interfaces on the sensor. You configured the interfaces when you initialized the sensor with the **setup** command, but if you need to change or add anything to your interface configuration, use the following procedures. For the easiest way to configure interfaces, see Initializing the Sensor, page 3-2.

This chapter contains the following sections:

Understanding Interfaces

The sensor interfaces are named according to the maximum speed and physical location of the interface. The physical location consists of a port number and a slot number. All interfaces that are built-in on the sensor motherboard are in slot 0, and the PCI expansion slots are numbered beginning with slot 1 for the bottom slot with the slot numbers increasing from bottom to top. Interfaces with a given slot are numbered beginning with port 0 for the right port with the port numbers increasing from right to left. For example, GigabitEthernet2/1 supports a maximum speed of 1 Gigabit and is the second-from-the-right interface in the second-from-the bottom PCI expansion slot. IPS-4240 and IPS-4255 are exceptions to this rule. The command and control interface on these sensors is called Management0/0 rather than GigabitEthernet0/0.

There are three interface roles:

- Command and control
- Sensing
- Alternate TCP reset

There are restrictions on which roles you can assign to specific interfaces and some interfaces have multiple roles. You can configure any sensing interface to any other sensing interface as its TCP reset interface. The TCP reset interface can also serve as an IDS (promiscuous) sensing interface at the same time. The following restrictions apply:

- Because NM-CIDS and AIP-SSM only have one sensing interface, you cannot configure a TCP reset interface.
- Because of hardware limitations on the Catalyst switch, both of the IDSM-2 sensing interfaces are permanently configured to use System0/1 as the TCP reset interface.
- The TCP reset interface that is assigned to a sensing interface has no effect in inline interface or inline VLAN pair mode, because TCP resets are always sent on the sensing interfaces in those modes.

This section contains the following topics:

- Command and Control Interface, page 5-2
- Sensing Interfaces, page 5-3
- Interface Support, page 5-3
- TCP Reset Interfaces, page 5-6
- Hardware Bypass Mode, page 5-7
- Configuration Sequence, page 5-9
- Interface Configuration Restrictions, page 5-10

Command and Control Interface

The command and control interface has an IP address and is used for configuring the sensor. It receives security and status events from the sensor and queries the sensor for statistics.

The command and control interface is permanently enabled. It is permanently mapped to a specific physical interface, which depends on the specific model of sensor. You cannot use the command and control interface as either a sensing or alternate TCP reset interface.

Table 5-1 lists the command and control interfaces for each sensor.

Table 5-1 Command and Control Interfaces

Sensor	Command and Control Interface
IDS-4210	FastEthernet0/1
IDS-4215	FastEthernet0/0
IDS-4235	GigabitEthernet0/1
IDS-4250	GigabitEthernet0/1
IPS-4240	Management0/0
IPS-4255	Management0/0
IPS-4260	Management0/0
NM-CIDS	FastEthernet0/0
AIP-SSM-10	GigabitEthernet0/0

Table 5-1 Command and Control Interfaces (continued)

Sensor	Command and Control Interface
AIP-SSM-20	GigabitEthernet0/0
IDSM-2	GigabitEthernet0/2

Sensing Interfaces

Sensing interfaces are used by the sensor to analyze traffic for security violations. A sensor has one or more sensing interfaces depending on the sensor. For the number and type of sensing interfaces available for each sensor, see Interface Support, page 5-3.

Sensing interfaces can operate individually in promiscuous mode or you can pair them to create inline interfaces for inline sensing mode. For more information, see Understanding Promiscuous Mode, page 5-14, Understanding Inline Interface Mode, page 5-15, and Understanding Inline VLAN Pair Mode, page 5-17.

Note On appliances, all sensing interfaces are disabled by default. You must enable them to use them. On modules, the sensing interfaces are permanently enabled.

Some appliances support optional PCI interface cards that add sensing interfaces to the sensor. You must insert or remove these optional cards while the sensor is powered off. The sensor detects the addition or removal of a supported interface card. If you remove an optional PCI card, some of the interface configuration is deleted, such as the speed, duplex, description string, enabled/disabled state of the interface, and any inline interface pairings. These settings are restored to their default settings when the card is reinstalled. However, the assignment of promiscuous and inline interfaces to the Analysis Engine is not deleted from the Analysis Engine configuration, but is ignored until those cards are reinserted and you create the inline interface pairs again. For more information, see Assigning Interfaces to the Virtual Sensor, page 5-24.

Interface Support

Table 5-2 describes the interface support for appliances and modules running IPS 5.1:

Table 5-2 Interface Support

Base Chassis	Added PCI Cards	Interfaces Supporting Inline VLAN Pairs (Sensing Ports)	Combinations Supporting Inline Interface Pairs	Interfaces Not Supporting Inline (Command and Control Port)
IDS-4210	—	FastEthernet0/0	N/A	FastEthernet0/1
IDS-4215	—	FastEthernet0/1	N/A	FastEthernet0/0

Table 5-2 Interface Support (continued)

Base Chassis	Added PCI Cards	Interfaces Supporting Inline VLAN Pairs (Sensing Ports)	Combinations Supporting Inline Interface Pairs	Interfaces Not Supporting Inline (Command and Control Port)
IDS-4215	4FE	FastEthernet0/1 FastEthernetS/0[1] FastEthernetS/1 FastEthernetS/2 FastEthernetS/3	1/0<->1/1 1/0<->1/2 1/0<->1/3 1/1<->1/2 1/1<->1/3 1/2<->1/3 0/1<->1/0 0/1<->1/1 0/1<->1/2 0/1<->1/3	FastEthernet0/0
IDS-4235	—	GigabitEthernet0/0	N/A	GigabitEthernet0/1
IDS-4235	4FE	GigabitEthernet0/0 FastEthernetS/0 FastEthernetS/1 FastEthernetS/2 FastEthernetS/3	1/0<->1/1 1/0<->1/2 1/0<->1/3 1/1<->1/2 1/1<->1/3 1/2<->1/3	GigabitEthernet0/1
IDS-4235	TX (GE)	GigabitEthernet0/0 GigabitEthernet1/0 GigabitEthernet2/0	0/0<->1/0 0/0<->2/0	GigabitEthernet0/1
IDS-4250	—	GigabitEthernet0/0	N/A	GigabitEthernet0/1
IDS-4250	4FE	GigabitEthernet0/0 FastEthernetS/0 FastEthernetS/1 FastEthernetS/2 FastEthernetS/3	1/0<->1/1 1/0<->1/2 1/0<->1/3 1/1<->1/2 1/1<->1/3 1/2<->1/3	GigabitEthernet0/1
IDS-4250	TX (GE)	GigabitEthernet0/0 GigabitEthernet1/0 GigabitEthernet2/0	0/0<->1/0 0/0<->2/0	GigabitEthernet0/1
IDS-4250	SX	GigabitEthernet0/0 GigabitEthernet1/0	N/A	GigabitEthernet0/1
IDS-4250	SX + SX	GigabitEthernet0/0 GigabitEthernet1/0 GigabitEthernet2/0	1/0<->2/0	GigabitEthernet0/1
IDS-4250	XL	GigabitEthernet0/0 GigabitEthernet2/0 GigabitEthernet2/1	2/0<->2/1	GigabitEthernet0/1
IDSM-2	—	GigabitEthernet0/7 GigabitEthernet0/8	0/7<->0/8	GigabitEthernet0/2

Table 5-2 Interface Support (continued)

Base Chassis	Added PCI Cards	Interfaces Supporting Inline VLAN Pairs (Sensing Ports)	Combinations Supporting Inline Interface Pairs	Interfaces Not Supporting Inline (Command and Control Port)
IPS-4240	—	GigabitEthernet0/0 GigabitEthernet0/1 GigabitEthernet0/2 GigabitEthernet0/3	0/0<->0/1 0/0<->0/2 0/0<->0/3 0/1<->0/2 0/1<->0/3 0/2<->0/3	Management0/0
IPS-4255	—	GigabitEthernet0/0 GigabitEthernet0/1 GigabitEthernet0/2 GigabitEthernet0/3	0/0<->0/1 0/0<->0/2 0/0<->0/3 0/1<->0/2 0/1<->0/3 0/2<->0/3	Management0/0
IPS-4260	—	GigabitEthernet0/1	N/A	Management0/0
IPS-4260	4GE-BP	GigabitEthernet0/1		Management0/0
	Slot 1	GigabitEthernet2/0 GigabitEthernet2/1 GigabitEthernet2/2 GigabitEthernet2/3	2/0<->2/1[2] 2/2<->2/3	
	Slot 2	GigabitEthernet3/0 GigabitEthernet3/1 GigabitEthernet3/2 GigabitEthernet3/3	3/0<->3/1 3/2<->3/3	
IPS-4260	2SX	GigabitEthernet0/1	All sensing ports can be paired together	Management0/0
	Slot 1	GigabitEthernet2/0 GigabitEthernet2/1 GigabitEthernet2/2 GigabitEthernet2/3		
	Slot 2	GigabitEthernet3/0 GigabitEthernet3/1 GigabitEthernet3/2 GigabitEthernet3/3		
NM-CIDS	—	None	N/A	All

Table 5-2 Interface Support (continued)

Base Chassis	Added PCI Cards	Interfaces Supporting Inline VLAN Pairs (Sensing Ports)	Combinations Supporting Inline Interface Pairs	Interfaces Not Supporting Inline (Command and Control Port)
AIP-SSM-10	—	GigabitEthernet0/1 by security context instead of VLAN pair or inline interface pair	GigabitEthernet0/1 by security context instead of VLAN pair or inline interface pair	GigabitEthernet0/0
AIP-SSM-20	—	GigabitEthernet0/1 by security context instead of VLAN pair or inline interface pair	GigabitEthernet0/1 by security context instead of VLAN pair or inline interface pair	GigabitEthernet0/0

[1] You can install the 4FE card in either slot 1 or 2. S indicates the slot number, which can be either 1 or 2.

[2] You can pair any two sensing ports together if you are not using the hardware bypass feature.

TCP Reset Interfaces

This section explains the TCP reset interfaces and when to use them. It contains the following topics:

- Understanding Alternate TCP Reset Interfaces, page 5-6
- Designating the Alternate TCP Reset Interface, page 5-7

Understanding Alternate TCP Reset Interfaces

You can configure sensors to send TCP reset packets to try to reset a network connection between an attacker host and its intended target host. In some installations when the interface is operating in promiscuous mode, the sensor may not be able to send the TCP reset packets over the same sensing interface on which the attack was detected. In such cases, you can associate the sensing interface with an alternate TCP reset interface and any TCP resets that would otherwise be sent on the sensing interface when it is operating in promiscuous mode, are instead sent out on the associated alternate TCP reset interface. For more information, see Designating the Alternate TCP Reset Interface, page 5-7.

If a sensing interface is associated with an alternate TCP reset interface, that association applies when the sensor is configured for promiscuous mode but is ignored when the sensing interface is configured for inline mode.

With the exception of IDSM-2, any sensing interface can serve as the alternate TCP reset interface for another sensing interface. The alternate TCP reset interface on IDSM-2 is fixed because of hardware limitation.

Table 5-3 lists the alternate TCP reset interfaces.

Table 5-3 Alternate TCP Reset Interfaces

Sensor	Alternate TCP Reset Interface
IDS-4210	None[1]
IDS-4215	Any sensing interface

Table 5-3 Alternate TCP Reset Interfaces

Sensor	Alternate TCP Reset Interface
IDS-4235	Any sensing interface
IDS-4250	Any sensing interface
IPS-4240	Any sensing interface
IPS-4255	Any sensing interface
IPS-4260	Any sensing interface
NM-CIDS	None[2]
AIP-SSM-10	None[3]
AIP-SSM-20	None[4]
IDSM-2	System0/1[5]

[1] There is only one sensing interface on IDS-4210.
[2] There is only one sensing interface on NM-CIDS.
[3] There is only one sensing interface on AIP-SSM-10.
[4] There is only one sensing interface on AIP-SSM-20.
[5] This is an internal interface on the Catalyst backplane.

Designating the Alternate TCP Reset Interface

You need to designate an alternate TCP reset interface in the following situations:

- When a switch is being monitored with either SPAN or VACL capture and the switch does not accept incoming packets on the SPAN or VACL capture port.
- When a switch is being monitored with either SPAN or VACL capture for multiple VLANs, and the switch does not accept incoming packets with 802.1q headers.

  Note The TCP resets need 802.1q headers to tell which VLAN the resets should be sent on.

- When a network tap is used for monitoring a connection.

  Note Taps do not permit incoming traffic from the sensor.

  You can only assign a sensing interface as an alternate TCP reset interface. You cannot configure the management interface as an alternate TCP reset interface.

Hardware Bypass Mode

In addition to IPS 5.1 software bypass, IPS-4260 also supports hardware bypass.

This section describes the hardware bypass card and its configuration restrictions. For the procedure for installing and removing the hardware bypass card, refer to Installing and Removing PCI Cards.

This section contains the following topics:

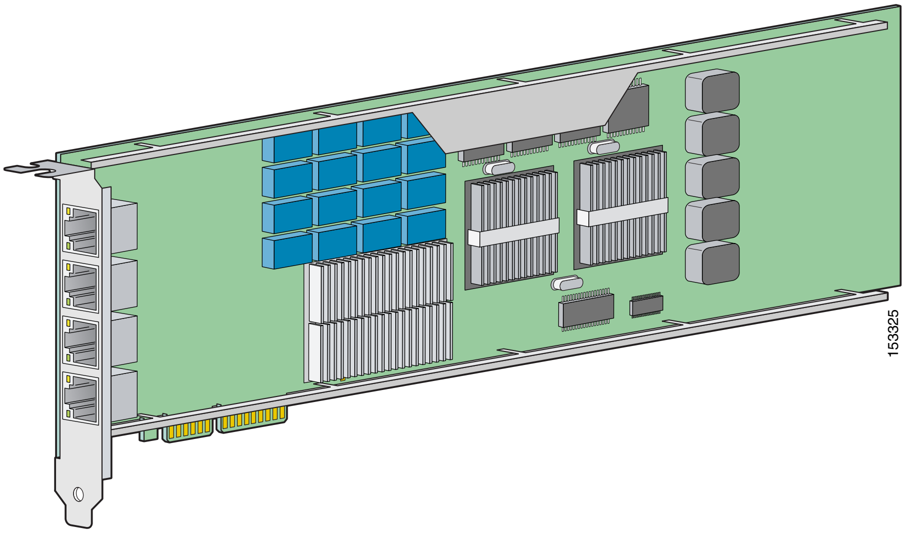
- Hardware Bypass Card, page 5-8
- Hardware Bypass Configuration Restrictions, page 5-9

Hardware Bypass Card

IPS-4260 supports the Intel 4-port PCI-Express card (part number IPS-4GE-BP-INT=) with hardware bypass. This 4GE bypass interface card supports hardware bypass only between ports 0 and 1 and between ports 2 and 3.

Figure 5-1 shows the 4GE bypass interface card.

Figure 5-1 4GE Bypass Interface Card



Hardware bypass complements the existing software bypass feature in IPS 5.1. For more information on software bypass mode, see Inline Bypass Mode, page 5-22. The following conditions apply to hardware bypass and software bypass on IPS-4260:

- When bypass is set to OFF, software bypass is not active.

  For each inline interface for which hardware bypass is available, the component interfaces are set to disable the fail-open capability. If SensorApp fails, the sensor is powered off, reset, or if the NIC interface drivers fail or are unloaded, the paired interfaces enter the fail-closed state (no traffic flows through inline interface or inline VLAN subinterfaces).

- When bypass is set to ON, software bypass is active.

  Software bypass forwards packets between the paired physical interfaces in each inline interface and between the paired VLANs in each inline VLAN subinterface. For each inline interface on which hardware bypass is available, the component interfaces are set to standby mode. If the sensor is powered off, reset, or if the NIC interfaces fail or are unloaded, those paired interfaces enter fail-open state in hardware. Any other inline interfaces enter fail-closed state.

- When bypass is set to AUTO (traffic flows without inspection), software bypass is activated if sensorApp fails.

  For each inline interface on which hardware bypass is available, the component interfaces are set to standby mode. If the sensor is powered off, reset, or if the NIC interfaces fail or are unloaded, those paired interfaces enter fail-open state in hardware. Any other inline interfaces enter the fail-closed state.

Note To test fail-over, set the bypass mode to ON or AUTO, create one or more inline interfaces and power down the sensor and verify that traffic still flows through the inline path.

Hardware Bypass Configuration Restrictions

To use the hardware bypass feature on the 4GE bypass interface card, you must pair interfaces to support the hardware design of the card. If you create an inline interface that pairs a hardware-bypass-capable interface with an interface that violates one or more of the hardware-bypass configuration restrictions, hardware bypass is deactivated on the inline interface and you receive a warning message similar to the following:

```
Hardware bypass functionality is not available on Inline-interface pair0.
Physical-interface GigabitEthernet1/0 is capable of performing hardware bypass only when
paired with GigabitEthernet1/1, and both interfaces are enabled and configured with the
same speed and duplex settings.
```

The following configuration restrictions apply to hardware bypass:

- The 4-port bypass card is only supported on IPS-4260.
- Fail-open hardware bypass only works on inline interfaces (interface pairs), not on inline VLAN pairs.
- Fail-open hardware bypass is available on an inline interface if all of the following conditions are met:
  - Both of the physical interfaces support hardware bypass.
  - Both of the physical interfaces are on the same interface card.
  - The two physical interfaces are associated in hardware as a bypass pair.
  - The speed and duplex settings are identical on the physical interfaces.
  - Both of the interfaces are administratively enabled.

Configuration Sequence

Follow these steps to configure interfaces on the sensor:

1. Configure the physical interface settings (speed, duplex, and admin state).

   For the procedure, see Configuring Physical Interfaces, page 5-11.

2. Create or delete inline interfaces and/or inline VLAN subinterfaces, and set the inline bypass mode.

   For more information, see Inline Interface Mode, page 5-15, Inline VLAN Pair Mode, page 5-17, and Inline Bypass Mode, page 5-22.

3. Assign the physical, subinterfaces, and inline interfaces to the virtual sensor.

   For the procedure, see Assigning Interfaces to the Virtual Sensor, page 5-24.

Interface Configuration Restrictions

For hardware bypass interface configuration restrictions, see Hardware Bypass Mode, page 5-7.

The following restrictions apply to configuring interfaces on the sensor:

- Physical Interfaces
  - On modules (IDSM-2, NM-CIDS, AIP-SSM-10, and AIP-SSM-20) and IPS-4240, IPS-4255, and IPS-4260, all backplane interfaces have fixed speed, duplex, and state settings. These settings are protected in the default configuration on all backplane interfaces.
  - For nonbackplane FastEthernet interfaces the valid speed settings are 10 Mbps, 100 Mbps, and auto. Valid duplex settings are full, half, and auto.
  - For Gigabit fiber interfaces (1000-SX and XL on the IDS-4250), valid speed settings are 1000 Mbps and auto.
  - For Gigabit copper interfaces (1000-TX on the IDS-4235, IDS-4250, IPS-4240, IPS-4255, and IPS-4260), valid speed settings are 10 Mbps, 100 Mbps, 1000 Mbps, and auto. Valid duplex settings are full, half, and auto.
  - For Gigabit (copper or fiber) interfaces, if the speed is configured for 1000 Mbps, the only valid duplex setting is auto.
  - The command and control interface cannot also serve as a sensing interface.
- Inline Interface Pairs
  - Inline interface pairs can contain any combination of sensing interfaces regardless of the physical interface type (copper versus fiber), speed, or duplex settings of the interface. However, pairing interfaces of different media type, speeds, and duplex settings may not be fully tested or supported. For more information, see Interface Support, page 5-3.
  - The command and control interface cannot be a member of an inline interface pair.
  - You cannot pair a physical interface with itself in an inline interface pair.
  - A physical interface can be a member of only one inline interface pair.
  - You can only configure bypass mode and create inline interface pairs on sensor platforms that support inline mode.
  - A physical interface cannot be a member of an inline interface pair unless the subinterface mode of the physical interface is **none**.
- Inline VLAN Interface Pairs
  - You cannot pair a VLAN with itself.
  - For a given sensing interface, a VLAN can be a member of only one inline VLAN pair. However, a given VLAN can be a member of an inline VLAN pair on more than one sensing interface.
  - The order in which you specify the VLANs in an inline VLAN pair is not significant.
  - A sensing interface in inline VLAN pair mode can have from 1 to 255 inline VLAN pairs.
- Alternate TCP Reset Interface:
  - You can only assign the alternate TCP reset interface to a sensing interface. You cannot configure the command and control interface as an alternate TCP reset interface. The alternate TCP reset interface option is set to **none** as the default and is protected for all interfaces except the sensing interfaces.

- You can assign the same physical interface as an alternate TCP reset interface for multiple sensing interfaces.
- A physical interface can serve as both a sensing interface and an alternate TCP reset interface.
- The command and control interface cannot serve as the alternate TCP reset interface for a sensing interface.
- A sensing interface cannot serve as its own alternate TCP reset interface.
- You can only configure interfaces that are capable of TCP resets as alternate TCP reset interfaces.

  Note The exception to this restriction is the IDSM-2. The alternate TCP reset interface assignments for both sensing interfaces is System0/1 (protected).

Configuring Physical Interfaces

Note For information on what you need to configure if you are using the hardware bypass card on IPS-4260, see Hardware Bypass Configuration Restrictions, page 5-9.

Use the **physical-interfaces** *interface_name* command in the service interface submode to configure promiscuous interfaces. The interface name is FastEthernet or GigabitEthernet. For a list of possible interfaces for your sensor, see Interface Support, page 5-3.

Note AIP-SSM is configured for promiscuous mode from the ASA CLI and not from the IPS CLI. For the procedure, see Sending Traffic to AIP-SSM, page 14-2.

The following options apply:

- **admin-state {enabled | disabled}**—The administrative link state of the interface, whether the interface is enabled or disabled.

  Note On all backplane sensing interfaces on all modules (IDSM-2 NM-CIDS, and AIP-SSM), **admin-state** is set to enabled and is protected (you cannot change the setting). The **admin-state** has no effect (and is protected) on the command and control interface. It only affects sensing interfaces. The command and control interface does not need to be enabled because it cannot be monitored.

- **alt-tcp-reset-interface**—Sends TCP resets out an alternate interface when this interface is used for promiscuous monitoring and the reset action is triggered by a signature firing. For more information on the alternate TCP reset interface, see Understanding Alternate TCP Reset Interfaces, page 5-6, and Designating the Alternate TCP Reset Interface, page 5-7.

  Note You can only assign a sensing interface as an alternate TCP reset interface. You cannot configure the management interface as an alternate TCP reset interface.

Note This option is protected on modules (IDSM-2 NM-CIDS, and AIP-SSM) and appliances that only have one sensing interface (IDS-4210, IDS-4215,IDS-4235, and IDS-4250 without any additional NIC cards).

  - *interface_name*—The name of the interface on which TCP resets should be sent when this interface is used for promiscuous monitoring and the reset action is triggered by a signature firing. This setting is ignored when this interface is a member of an inline interface.
  - **none** —Disables the use of an alternate TCP reset interface. TCP resets triggered by the reset action when in promiscuous mode will be sent out of this interface instead.
- **default**—Sets the value back to the system default setting.
- **description**—Your description of the promiscuous interface.
- **duplex**—The duplex setting of the interface.
  - **auto**—Sets the interface to auto negotiate duplex.
  - **full**—Sets the interface to full duplex.
  - **half**—Sets the interface to half duplex.

  Note The **duplex** option is protected on all modules.

- **no**—Remove an entry or selection setting.
- **speed**—The speed setting of the interface.
  - **auto**—Sets the interface to auto negotiate speed.
  - **10**—Sets the interface to 10 MB (for TX interfaces only).
  - **100**—Sets the interface to 100 MB (for TX interfaces only).
  - **1000**—Sets the interface to 1 GB (for Gigabit interfaces only).

  Note The **speed** option is protected on all modules.

To configure the promiscuous interface settings on the sensor, follow these steps:

Step 1 Log in to the CLI using an account with administrator privileges.

Step 2 Enter interface submode:

```
sensor# configure terminal
sensor(config)# service interface
```

Step 3 Display the list of available interfaces:

```
sensor(config-int)# physical-interfaces ?
GigabitEthernet0/0     GigabitEthernet0/0 physical interface.
GigabitEthernet0/1     GigabitEthernet0/1 physical interface.
GigabitEthernet0/2     GigabitEthernet0/2 physical interface.
GigabitEthernet0/3     GigabitEthernet0/3 physical interface.
Management0/0          Management0/0 physical interface.
sensor(config-int)# physical-interfaces
```

Step 4 Specify the interface for promiscuous mode:

```
sensor(config-int)# physical-interfaces GigabitEthernet0/2
```

Step 5 Enable the interface:

```
sensor(config-int-phy)# admin-state enabled
```

The interface must be assigned to the virtual sensor (see Assigning Interfaces to the Virtual Sensor, page 5-24) and enabled to monitor traffic.

Step 6 Add a description of this interface:

```
sensor(config-int-phy)# description INT1
```

Step 7 Configure the duplex settings:

```
sensor(config-int-phy)# duplex full
```

This option is not available on modules.

Step 8 Configure the speed:

```
sensor(config-int-phy)# speed 1000
```

This option is not available on modules.

Step 9 Enable TCP resets for this interface if desired:

```
sensor(config-int-phy)# alt-tcp-reset-interface interface-name GigabitEthernet2/0
```

Step 10 Repeat Steps 4 through 9 for any other interfaces you want to designate as promiscuous interfaces.

Step 11 Verify the settings:

Note Make sure the `subinterface-type` is *none*, the default. You use the **subinterface-type** command to configure inline VLAN pairs. For more information, see Configuring Inline VLAN Pairs, page 5-18.

```
sensor(config-int-phy)# show settings
   <protected entry>
   name: GigabitEthernet0/2
   -----------------------------------------------
      media-type: tx <protected>
      description: INT1 default:
      admin-state: enabled default: disabled
      duplex: full default: auto
      speed: 1000 default: auto
     alt-tcp-reset-interface
     -----------------------------------------------
        interface-name: GigabitEthernet2/0
     -----------------------------------------------
     subinterface-type
     -----------------------------------------------
        none
        -----------------------------------------------
        -----------------------------------------------
     -----------------------------------------------
  -----------------------------------------------
sensor(config-int-phy)#
```

Step 12 To remove TCP resets from an interface:

```
sensor(config-int-phy)# alt-tcp-reset-interface none
```

Step 13 Verify the settings:

```
sensor(config-int-phy)# show settings
   <protected entry>
   name: GigabitEthernet0/0
   -----------------------------------------------
      media-type: tx <protected>
      description: <defaulted>
      admin-state: disabled <protected>
      duplex: auto <defaulted>
      speed: auto <defaulted>
      alt-tcp-reset-interface
      -----------------------------------------------
         none
         -----------------------------------------------
         -----------------------------------------------
      -----------------------------------------------
   -----------------------------------------------
sensor(config-int-phy)#
```

Step 14 Exit interface submode:

```
sensor(config-int-phy)# exit
sensor(config-int)# exit
Apply Changes:?[yes]:
```

Step 15 Press **Enter** to apply the changes or enter **`no`** to discard them.

Promiscuous Mode

This section describes promiscuous mode on the sensor, and contains the following topics:

- Understanding Promiscuous Mode, page 5-14
- Configuring Promiscuous Mode, page 5-15

Understanding Promiscuous Mode

In promiscuous mode, packets do not flow through the sensor. The sensor analyzes a copy of the monitored traffic rather than the actual forwarded packet. The advantage of operating in promiscuous mode is that the sensor does not affect the packet flow with the forwarded traffic. The disadvantage of operating in promiscuous mode, however, is the sensor cannot stop malicious traffic from reaching its intended target for certain types of attacks, such as atomic attacks (single-packet attacks). The response actions implemented by promiscuous sensor devices are post-event responses and often require assistance from other networking devices, for example, routers and firewalls, to respond to an attack. While such response actions can prevent some classes of attacks, in atomic attacks the single packet has the chance of reaching the target system before the promiscuous-based sensor can apply an ACL modification on a managed device (such as a firewall, switch, or router).

Configuring Promiscuous Mode

By default, all sensing interfaces are in promiscuous mode. To change an interface from inline mode to promiscuous mode, delete any inline interface that contains that interface and delete any inline VLAN pair subinterfaces of that interface from the interface configuration.

Inline Interface Mode

This section describes inline mode on the sensor, and contains the following topics:

- Understanding Inline Interface Mode, page 5-15
- Configuring Inline Interface Pairs, page 5-15

Understanding Inline Interface Mode

Operating in inline interface mode puts the IPS directly into the traffic flow and affects packet-forwarding rates making them slower by adding latency. This allows the sensor to stop attacks by dropping malicious traffic before it reaches the intended target, thus providing a protective service. Not only is the inline device processing information on layers 3 and 4, but it is also analyzing the contents and payload of the packets for more sophisticated embedded attacks (layers 3 to 7). This deeper analysis lets the system identify and stop and/or block attacks that would normally pass through a traditional firewall device.

In inline interface mode, a packet comes in through the first interface of the pair on the sensor and out the second interface of the pair. The packet is sent to the second interface of the pair unless that packet is being denied or modified by a signature.

Note You can configure AIP-SSM to operate inline even though it has only one sensing interface.

Note If the paired interfaces are connected to the same switch, you should configure them on the switch as access ports with different access VLANs for the two ports. Otherwise, traffic does not flow through the inline interface.

Configuring Inline Interface Pairs

Note For information on what you need to configure if you are using the hardware bypass card on IPS-4260, see Hardware Bypass Configuration Restrictions, page 5-9.

Use the **inline-interfaces** command in the service interface submode to configure inline interfaces.

Note AIP-SSM is configured for inline interface mode from the ASA CLI and not from the IPS CLI. For the procedure, see Sending Traffic to AIP-SSM, page 14-2.

The following options apply:

- **inline-interfaces**—Name of the logical inline interface pair.
- **default**—Sets the value back to the system default setting.
- **description**—Your description of the inline interface pair.
- **interface1**—The first interface in the inline interface pair.
- **interface2**—The second interface in the inline interface pair.
- **no**—Removes an entry or selection setting.

To configure the inline interface settings, follow these steps:

Step 1 Log in to the CLI using an account with administrator privileges.

Step 2 Enter interface submode:

```
sensor# configure terminal
sensor(config)# service interface
sensor(config-int)#
```

Step 3 Verify that the subinterface mode is "none" for both of the physical interfaces you are pairing in the inline interface:

```
sensor(config-int)# show settings
   physical-interfaces (min: 0, max: 999999999, current: 2)
   -----------------------------------------------
      <protected entry>
      name: GigabitEthernet0/0 <defaulted>
      -----------------------------------------------
         media-type: tx <protected>
         description: <defaulted>
         admin-state: disabled <protected>
         duplex: auto <defaulted>
         speed: auto <defaulted>
         alt-tcp-reset-interface
         -----------------------------------------------
            none
            -----------------------------------------------
            -----------------------------------------------
         -----------------------------------------------
         subinterface-type
         -----------------------------------------------
            none
            -----------------------------------------------
            -----------------------------------------------
         -----------------------------------------------
      -----------------------------------------------
```

Step 4 Name the inline pair:

```
sensor(config-int)# inline-interfaces PAIR1
```

Step 5 Display the available interfaces:

```
sensor(config-int)# interface1?
GigabitEthernet0/0     GigabitEthernet0/0 physical interface.
GigabitEthernet0/1     GigabitEthernet0/1 physical interface.
GigabitEthernet0/2     GigabitEthernet0/2 physical interface.
GigabitEthernet0/3     GigabitEthernet0/3 physical interface.
Management0/0          Management0/0 physical interface.
```

Step 6 Configure two interfaces into a pair:

```
sensor(config-int-inl)# interface1 GigabitEthernet0/0
sensor(config-int-inl)# interface2 GigabitEthernet0/1
```

Step 7 Add a description of the interface pair:

```
sensor(config-int-inl)# description pairs interfaces Gig0/0 and Gig0/1
```

Step 8 Repeat Steps 4 through 7 for any other interfaces that you want to configure into inline interface pairs.

Step 9 Verify the settings:

```
sensor(config-int-inl)# show settings
   name: PAIR1
   -----------------------------------------------
      description: PAIR1 = Gig0/0 & Gig0/1 default:
      interface1: GigabitEthernet0/0
      interface2: GigabitEthernet0/1
   -----------------------------------------------
```

Step 10 To remove an inline interface pair and return the interfaces to promiscuous mode:

```
sensor(config-int-inl)# exit
sensor(config-int)#
```

Step 11 Enable the interfaces assigned to the interface pair:

```
sensor(config-int)# physical-interfaces GigabitEthernet0/0
sensor(config-int-phy)# admin-state enabled
sensor(config-int-phy)# exit
sensor(config-int)# physical-interfaces GigabitEthernet0/1
sensor(config-int-phy)# admin-state enabled
sensor(config-int-phy)# exit
sensor(config-int)#
```

Step 12 Exit interface configuration submode:

```
sensor(config-int)# exit
Apply Changes:?[yes]:
```

Step 13 Press **Enter** to apply the changes or enter `no` to discard them.

Inline VLAN Pair Mode

This section describes inline VLAN pair mode and how to configure inline VLAN pairs. It contains the following topics:

- Understanding Inline VLAN Pair Mode, page 5-17
- Configuring Inline VLAN Pairs, page 5-18

Understanding Inline VLAN Pair Mode

Note For IPS-4260, fail-open hardware bypass is not supported on inline VLAN pairs. For more information, see Hardware Bypass Configuration Restrictions, page 5-9.

You can associate VLANs in pairs on a physical interface. Packets received on one of the paired VLANs are analyzed and then forwarded to the other VLAN in the pair. Inline VLAN pairs are supported on all sensors that are compatible with IPS 5.1 except NM-CIDS, AIP-SSM-10, and AIP-SSM-20.

Inline VLAN pair mode is an active sensing mode where a sensing interface acts as an 802.1q trunk port, and the sensor performs VLAN bridging between pairs of VLANs on the trunk. The sensor inspects the traffic it receives on each VLAN in each pair, and can either forward the packets on the other VLAN in the pair, or drop the packet if an intrusion attempt is detected. You can configure an IPS sensor to simultaneously bridge up to 255 VLAN pairs on each sensing interface. The sensor replaces the VLAN ID field in the 802.1q header of each received packet with the ID of the egress VLAN on which the sensor forwards the packet. The sensor drops all packets received on any VLANs that are not assigned to inline VLAN pairs.

Configuring Inline VLAN Pairs

Use the **physical-interfaces** *interface_name* command in the service interface submode to configure inline VLAN pairs. The interface name is FastEthernet or GigabitEthernet.

The following options apply:

- **admin-state {enabled | disabled}**—The administrative link state of the interface, whether the interface is enabled or disabled.

  Note On all backplane sensing interfaces on all modules (IDSM-2 NM-CIDS, and AIP-SSM), **admin-state** is set to enabled and is protected (you cannot change the setting). The **admin-state** has no effect (and is protected) on the command and control interface. It only affects sensing interfaces. The command and control interface does not need to be enabled because it cannot be monitored.

- **default**—Sets the value back to the system default setting.
- **description**—Your description of the interface.
- **duplex**—The duplex setting of the interface.
  - **auto**—Sets the interface to auto negotiate duplex.
  - **full**—Sets the interface to full duplex.
  - **half**—Sets the interface to half duplex.

  Note The **duplex** option is protected on all modules.

- **no**—Removes an entry or selection setting.

- **speed**—The speed setting of the interface.
  - **auto**—Sets the interface to auto negotiate speed.
  - **10**—Sets the interface to 10 MB (for TX interfaces only).
  - **100**—Sets the interface to 100 MB (for TX interfaces only).
  - **1000**—Sets the interface to 1 GB (for Gigabit interfaces only).

  Note The **speed** option is protected on all modules.

- **subinterface-type**—Specifies that the interface is a subinterface and what type of subinterface is defined.
  - **inline-vlan-pair**—Lets you define the subinterface as an inline VLAN pair.
  - **none**—No subinterfaces defined.
- **subinterface**—Defines the subinterface as an inline VLAN pair.
  - **vlan1**—The first VLAN in the inline VLAN pair.
  - **vlan2**—The second VLAN in the inline VLAN pair.

To configure the inline VLAN pair settings on the sensor, follow these steps:

Step 1 Log in to the CLI using an account with administrator privileges.

Step 2 Enter interface submode:

```
sensor# configure terminal
sensor(config)# service interface
sensor(config-int)#
```

Step 3 Verify if any inline interfaces exist (the subinterface type should read “none” if no inline interfaces have been configured):

```
sensor(config-int)# show settings
   physical-interfaces (min: 0, max: 999999999, current: 5)
   -----------------------------------------------
      <protected entry>
      name: GigabitEthernet0/0 <defaulted>
      -----------------------------------------------
         media-type: tx <protected>
         description: <defaulted>
         admin-state: disabled <defaulted>
         duplex: auto <defaulted>
         speed: auto <defaulted>
         alt-tcp-reset-interface
         -----------------------------------------------
            none
            -----------------------------------------------
            -----------------------------------------------
         -----------------------------------------------
         subinterface-type
         -----------------------------------------------
            none
            -----------------------------------------------
            -----------------------------------------------
         -----------------------------------------------
      -----------------------------------------------
      <protected entry>
      name: GigabitEthernet0/1 <defaulted>
```

```
-----------------------------------------------
   media-type: tx <protected>
   description: <defaulted>
   admin-state: disabled <defaulted>
   duplex: auto <defaulted>
   speed: auto <defaulted>
   alt-tcp-reset-interface
   -----------------------------------------------
      none
      -----------------------------------------------
      -----------------------------------------------
   -----------------------------------------------
   subinterface-type
   -----------------------------------------------
      none
      -----------------------------------------------
      -----------------------------------------------
   -----------------------------------------------
-----------------------------------------------
<protected entry>
name: GigabitEthernet0/2 <defaulted>
-----------------------------------------------
   media-type: tx <protected>
   description: <defaulted>
   admin-state: disabled <defaulted>
   duplex: auto <defaulted>
   speed: auto <defaulted>
   alt-tcp-reset-interface
   -----------------------------------------------
      none
      -----------------------------------------------
      -----------------------------------------------
   -----------------------------------------------
   subinterface-type
   -----------------------------------------------
      none
      -----------------------------------------------
      -----------------------------------------------
   -----------------------------------------------
-----------------------------------------------
<protected entry>
name: GigabitEthernet0/3 <defaulted>
-----------------------------------------------
   media-type: tx <protected>
   description: <defaulted>
   admin-state: disabled <defaulted>
   duplex: auto <defaulted>
   speed: auto <defaulted>
   alt-tcp-reset-interface
   -----------------------------------------------
      none
      -----------------------------------------------
      -----------------------------------------------
   -----------------------------------------------
   subinterface-type
   -----------------------------------------------
      none
      -----------------------------------------------
      -----------------------------------------------
   -----------------------------------------------
-----------------------------------------------
<protected entry>
name: Management0/0 <defaulted>
-----------------------------------------------
```

```
         media-type: tx <protected>
         description: <defaulted>
         admin-state: disabled <protected>
         duplex: auto <defaulted>
         speed: auto <defaulted>
         alt-tcp-reset-interface
         -----------------------------------------------
            none
            -----------------------------------------------
            -----------------------------------------------
         -----------------------------------------------
         subinterface-type
         -----------------------------------------------
            none
            -----------------------------------------------
            -----------------------------------------------
         -----------------------------------------------
      -----------------------------------------------
   -----------------------------------------------
   command-control: Management0/0 <protected>
   inline-interfaces (min: 0, max: 999999999, current: 0)
   -----------------------------------------------
   -----------------------------------------------
   bypass-mode: auto <defaulted>
   interface-notifications
   -----------------------------------------------
      missed-percentage-threshold: 0 percent <defaulted>
      notification-interval: 30 seconds <defaulted>
      idle-interface-delay: 30 seconds <defaulted>
   -----------------------------------------------
sensor(config-int)#
```

Step 4 If there are inline interfaces that are using this physical interface, remove them:

```
sensor(config-int)# no inline-interfaces interface_name
```

Step 5 Display the list of available interfaces:

```
sensor(config-int)# physical-interfaces ?
GigabitEthernet0/0     GigabitEthernet0/0 physical interface.
GigabitEthernet0/1     GigabitEthernet0/1 physical interface.
GigabitEthernet0/2     GigabitEthernet0/2 physical interface.
GigabitEthernet0/3     GigabitEthernet0/3 physical interface.
Management0/0          Management0/0 physical interface.
sensor(config-int)# physical-interfaces
```

Step 6 Specify an interface:

```
sensor(config-int)# physical-interfaces GigabitEthernet0/2
```

Step 7 Enable the interface:

```
sensor(config-int-phy)# admin-state enabled
```

The interface must be assigned to the virtual sensor (see Assigning Interfaces to the Virtual Sensor, page 5-24) and enabled to monitor traffic.

Step 8 Add a description of this interface:

```
sensor(config-int-phy)# description INT1
```

Step 9 Configure the duplex settings:

```
sensor(config-int-phy)# duplex full
```

This option is not available on modules.

Step 10 Configure the speed:

```
sensor(config-int-phy)# speed 1000
```

This option is not available on modules.

Step 11 Set up the inline VLAN pair:

```
sensor(config-int-phy)# subinterface-type inline-vlan-pair
sensor(config-int-phy-inl)# subinterface 1
sensor(config-int-phy-inl-sub)# vlan1 52
sensor(config-int-phy-inl-sub)# vlan2 53
```

Step 12 Add a description for the inline VLAN pair:

```
sensor(config-int-phy-inl-sub)# description pairs vlans 52 and 53
```

Step 13 Verify the inline VLAN pair settings:

```
sensor(config-int-phy-inl-sub)# show settings
   subinterface-number: 1
   -----------------------------------------------
      description: VLANpair1 default:
      vlan1: 52
      vlan2: 53
   -----------------------------------------------
sensor(config-int-phy-inl-sub)#
```

Step 14 Exit interface submode:

```
sensor(config-int-phy-inl-sub)# exit
sensor(config-int-phy-inl)# exit
sensor(config-int-phy)# exit
sensor(config-int)# exit
Apply Changes:?[yes]:
```

Step 15 Press **Enter** to apply the changes or enter **`no`** to discard them.

Inline Bypass Mode

This section describes inline bypass for sensors configured as inline interface and inline VLAN pairs, and contains the following topics:

- Understanding Inline Bypass Mode, page 5-22
- Configuring Bypass Mode, page 5-23

Understanding Inline Bypass Mode

Note For more information on using hardware bypass mode with software bypass mode, see Hardware Bypass Mode, page 5-7.

You can use inline bypass as a diagnostic tool and a failover protection mechanism. Normally, the sensor Analysis Engine performs packet analysis. When inline bypass is activated, Analysis Engine is bypassed, allowing traffic to flow through the inline interfaces and inline VLAN pairs without inspection. Inline bypass ensures that packets continue to flow through the sensor when the sensor processes are temporarily stopped for upgrades or when the sensor monitoring processes fail. There are three modes: on, off, and automatic. By default, bypass mode is set to automatic.

Caution There are security consequences when you put the sensor in bypass mode. When bypass mode is on, the traffic bypasses the sensor and is not inspected, therefore, the sensor cannot prevent malicious attacks.

Note The inline bypass functionality is implemented in software, so it only functions when the operating system is running. If the sensor is powered off or shut down, inline bypass does not work—traffic does not flow through the sensor.

Configuring Bypass Mode

Use the **bypass-mode** command in the service interface submode to configure bypass mode.

The following options apply:

- **off**—Turns off inline bypassing. Packet inspection is performed on inline data traffic. However, inline traffic is interrupted if Analysis Engine is stopped.
- **on**—Turns on inline bypassing. No packet inspection is performed on the traffic. Inline traffic continues to flow even if Analysis Engine is stopped.
- **auto**—Automatically begins bypassing inline packet inspection if Analysis Engine stops processing packets. This prevents data interruption on inline interfaces. This is the default.

Step 1 Log in to the CLI using an account with administrator privileges.

Step 2 Enter interface submode:

```
sensor# configure terminal
sensor(config)# service interface
```

Step 3 Configure bypass mode:

```
sensor(config-int)# bypass-mode off
```

Step 4 Verify the settings:

```
sensor(config-int)# show settings
-----------------------------------------------
 bypass-mode: off default: auto
 interface-notifications
 -----------------------------------------------
    missed-percentage-threshold: 0 percent <defaulted>
    notification-interval: 30 seconds <defaulted>
    idle-interface-delay: 30 seconds <defaulted>
 -----------------------------------------------
sensor(config-int)#
```

Step 5 Exit interface submode:

```
sensor(config-int)# exit
Apply Changes:?[yes]:
```

Step 6 Press **Enter** to apply the changes or enter `no` to discard them.

Assigning Interfaces to the Virtual Sensor

This section describes the virtual sensor and how to add interfaces to it. It contains the following topics:

- Overview, page 5-24
- Configuring Interfaces for the Virtual Sensor, page 5-24

Overview

The sensor can receive data inputs from one or many monitored data streams. These monitored data streams can either be physical interface ports or virtual interface ports. For example, a single sensor can monitor traffic from in front of the firewall and from behind the firewall. IPS 5.1 only supports one virtual sensor, so a single sensor policy and configuration are applied to all monitored data streams.

Be aware of the following limitation when adding interfaces to the sensor—the same traffic flow cannot traverse the sensor twice either through the same interface in inline mode or through separate monitored interfaces. If packets from the same traffic flow traverse the sensor twice, the virtual sensor interprets the packets as duplicates, which results in false positive alerts.

You can configure NAT to change the IP address to handle this limitation. NAT causes the sensor to treat the before and after translation packets as separate flows. For example, if a firewall is using NAT from its internal to external networks, the sensor can monitor both of these networks without problem.

You can assign interfaces, interface pairs, and VLAN pairs to the virtual sensor and you can change the description of the virtual sensor, but you cannot add a virtual sensor or change the virtual sensor name.

Configuring Interfaces for the Virtual Sensor

Use the **physical-interface** *interface_name* command in the virtual sensor submode to assign promiscuous interfaces to the virtual sensor. Use the **physical-interface** *interface_name* **subinterface-number** *subinterface_number* command in the virtual sensor submode to assign subinterfaces with inline VLAN pairs to the virtual sensor. Use the **logical-interface** *inline_interface_pair_name* command in the virtual sensor submode to assign inline interface pairs to the virtual sensor.

Make sure that you have created any inline interface pairs or inline VLAN pairs before assigning them to the virtual sensor.

To assign the interface to the virtual sensor, follow these steps:

Step 1 Log in to the CLI using an account with administrator privileges.

Step 2 Enter virtual sensor submode:

```
sensor# configure terminal
```

```
sensor(config)# service analysis-engine
sensor(config-ana)# virtual-sensor vs0
```

Step 3 Display the list of available interfaces:

```
sensor(config-ana-vir)# physical-interfaces ?
GigabitEthernet0/0     GigabitEthernet0/0 physical interface.
GigabitEthernet0/1     GigabitEthernet0/1 physical interface.
GigabitEthernet2/0     GigabitEthernet2/0 physical interface.
GigabitEthernet2/1     GigabitEthernet2/1 physical interface.
sensor(config-ana-vir)# physical-interfaces
```

Step 4 Assign the promiscuous mode interfaces to the virtual sensor:

```
sensor(config-ana-vir)# physical-interface GigabitEthernet2/0
```

Repeat Step 4 for all promiscuous mode interfaces.

Step 5 Assign the inline interface pairs to the sensor:

```
sensor(config-ana-vir)# logical-interface inline_interface_pair_name
```

Repeat Step 5 for all inline interface pair interfaces.

Step 6 Assign the subinterface with the inline VLAN pairs to the virtual sensor:

```
sensor(config-ana-vir)# physical-interface GigabitEthernet2/0 subinterface-number
subinterface_number
```

Repeat Step 6 for all subinterfaces with inline VLAN pairs.

Step 7 Exit analysis engine mode:

```
sensor(config-ana-vir)# exit
sensor(config-ana)# exit
sensor(config)#
Apply Changes:?[yes]:
```

Step 8 Press **Enter** to apply the changes or enter `no` to discard them.

Configuring Interface Notifications

You can configure the sensor to monitor the flow of packets across an interface and send notification if that flow changes (starts/stops) during a specified interval. You can configure the missed packet threshold within a specific notification interval and also configure the interface idle delay before a status event is reported.

Use the **interface-notifications** command in the service interface submode to configure traffic notifications.

The following options apply:

- **default**—Sets the value back to the system default setting.
- **idle-interface-delay**—The number of seconds an interface must be idle before sending a notification. The valid range is 5 to 3600. The default is 30 seconds.

- **missed-percentage-threshold**—The percentage of packets that must be missed during a specified interval before notification will be sent. The valid range is 0 to 100. The default is 0.
- **notification-interval**—Interval to check for missed packet percentage. The valid range is 5 to 3600. The default is 30 seconds

To configure the interface notification settings, follow these steps:

Step 1 Log in to the CLI using an account with administrator privileges.

Step 2 Enter global configuration mode:

```
sensor# configure terminal
```

Step 3 Enter interface submode:

```
sensor(config)# service interface
```

Step 4 Enter interface notifications submode:

```
sensor(config-int)# interface-notifications
```

Step 5 Configure the idle interface delay:

```
sensor(config-int-int)# idle-interface-delay 60
```

Step 6 Configure the missed percentage threshold:

```
sensor(config-int-int)# missed-percentage-threshold 1
```

Step 7 Configure the notification interval:

```
sensor(config-int-int)# notification-interval 60
```

Step 8 Verify the settings:

```
sensor(config-int-int)# show settings
   interface-notifications
   -----------------------------------------------
      missed-percentage-threshold: 1 percent default: 0
      notification-interval: 60 seconds default: 30
      idle-interface-delay: 60 seconds default: 30
   -----------------------------------------------
sensor(config-int-int)#
```

Step 9 Exit interface notifications submode:

```
sensor(config-int-int)# exit
sensor(config-int)# exit
Apply Changes:?[yes]:
```

Step 10 Press **Enter** to apply the changes or enter `no` to discard them.